New York Journal of Mathematics

New York J. Math. **22** (2016) 989–1020.

Divisibility sequences of polynomials and heights estimates

Bartosz Naskręcki

Abstract. In this note we compute a constant N that bounds the number of nonprimitive divisors in elliptic divisibility sequences over function fields of any characteristic. We improve a result of Ingram–Mahé–Silverman–Stange–Streng, 2012, and we show that the constant can be chosen independently of the specific point and to some extent of the specific curve, as predicted in loc. cit.

Contents

1. Introduction 989
2. Main theorems 991
3. Notation 992
4. Preliminaries 992
5. Arithmetic functions 995
6. Bounds on the canonical height 996
7. Characteristic 0 argument 998
8. Characteristic p argument 1003
9. Examples 1013
Acknowledgments 1018
References 1018

1. Introduction

Let E be an elliptic curve over the function field $K(C)$ of a smooth projective curve C of genus $g(C)$ over an algebraically closed field K. Let S be the Kodaira–Néron model of E, i.e. a smooth projective surface with a relatively minimal elliptic fibration $\pi : S \to C$ with a generic fibre E and a

Received April 24, 2015.

2010 *Mathematics Subject Classification.* Primary 11G05; Secondary 11B83 11C08 14H52.

Key words and phrases. Elliptic divisibility sequence, primitive divisor, elliptic surface, height of point.

The author was supported by the National Science Centre Poland research grant 2012/07/B/ST1/03541 and by the DFG grant Sto299/11-1 within the framework of the Priority Programme SPP 1489.

ISSN 1076-9803/2016

section $O : C \to S$, cf. [24, §1], [27, Chap. III, §3]. We always assume that π is not smooth. Let P be a point of infinite order in the Mordell–Weil group $E(K(C))$. To formulate the main problem we define a family of effective divisors $D_{nP} \in \mathrm{Div}(C)$ parametrized by natural numbers n. For each $n \in \mathbb{N}$ the divisor D_{nP} is the pullback of the image $\overline{O}$ of section O through the morphism $\sigma_{nP} : C \to S$ induced by the point nP

$$D_{nP} = \sigma_{nP}^*(\overline{O}).$$

We call such a family an *elliptic divisibility sequence*. We say that the divisor D_{nP} is *primitive* if the support of D_{nP} is *not* completely contained in the sum of supports of the divisors D_{mP} for all $m < n$. Otherwise we say that the divisor D_{nP} is *nonprimitive*.

The study of elliptic divisibility sequences dates back to the work of Morgan Ward [34, 35]. Silverman in [26] established that for elliptic divisibility sequences over $\mathbb{Q}$ the number of nonprimitive divisors is finite. This result was investigated further by several authors [4, 5, 10, 12, 15, 29]. In another direction Streng [31] generalized the primitive divisor theorems for curves with complex multiplication. Several authors studied also the question of existence of perfect powers in divisibility sequences, cf. [3, 6, 20]. In the context of elliptic divisibility sequences over function fields the finiteness of the set of nonprimitive divisors for elliptic curves over $\mathbb{Q}(t)$ was proved in [3]. In parallel such questions have been studied also for Lucas sequences [7]. In [28] common divisors of two distinct elliptic divisibility sequences were studied. For a general function field of a smooth curve in characteristic zero, the first general theorem about primitive divisors in elliptic divisibility sequences was proved in [11]. The authors of [11] ask the following question: *For a fixed elliptic curve E over a function field and a point P of infinite order is it possible to give an explicit upper bound for the value of a constant $N = N(E, P)$ such that for all $n \geq N$ the divisor D_{nP} in the elliptic divisibility sequence is primitive?*

Such a bound $N(E, P)$ always exists by [11, Thm. 5.5] but the proof does not indicate how to make the bound explicit or uniform with respect to E and P.

In this note we investigate the existence of uniform bounds for the number of nonprimitive divisors. In Section 2 we formulate our main theorems. There is a considerable difference between the formulation and proof of theorems in characteristic zero and positive so we do state them separately. In Section 3 we establish necessary notation that will be used through the paper. In Section 4 we gather basic facts about the canonical height function and the relation between the discriminant divisor of an elliptic curve and the Euler characteristic of the attached elliptic surface. The crux is the explicit recipe for the height function due to Shioda [24], that will be used in critical places to get the estimate on the number of nonprimitive divisors in the divisibility sequence. Section 5 contains a couple of properties of arithmetic functions

used in the proofs of main theorems. In Section 6 we discuss the analogue of Lang's conjecture on canonical height of points over function fields. We use the results of [9] and [19] to produce effective bounds for fields of arbitrary characteristic.

In Section 7 we explain a relatively simple proof of theorems formulated for function fields of characteristic 0. The main idea of the proof is to combine the explicit approach to height computations of [24] with the bounds for minimal heights of points proved in [9]. A crucial step in the proof relies on the formula that relates the Euler characteristic $\chi(S)$ to the sum of numbers that depended on the Kodaira types of singular fibres of π.

In Section 8 we prove the main theorems in positive characteristic. The main steps of the proof are similar to the characteristic 0 case, however there are significant differences due to the presence of inseparable multiplication by p map. In the last section we gather several examples for which we compute explicitly the exact number of nonprimitive divisors. We also explain how the main theorems fail in positive characteristic p for elliptic curves with p-map of inseparable degree p^2.

2. Main theorems

Our convention is to work with function fields $K(C)$ over algebraically closed field K of constants. However, the main theorems can be formulated for a smooth, projective geometrically irreducible curve C over a field K that is a number field or a finite field. In such a case, an elliptic curve E is defined over the field $K(C)$ and the elliptic surface $\pi : S \to C$ attached to $E/K(C)$ is a regular scheme S over K with a proper flat morphism π into C and such that its base change to the algebraic closure $\overline{K}$ is an elliptic surface in the usual sense. Every point $v \in C(\overline{K})$ corresponds to a normalized valuation of $\overline{K}(C)$. We say that v is a *primitive valuation* of D_{nP} when v is contained in the support of D_{nP} and does not belong to the support of any D_{mP} for $m < n$, cf. [11, Def. 5.4]. In this terminology we can say that D_{nP} is primitive if and only if it has a primitive valuation and similarly D_{nP} is nonprimitive whenever it does not have a primitive valuation.

From now on we assume that $K = \overline{K}$, unless otherwise specified. Let E be an elliptic curve over the field $K(C)$ with at least one fibre of bad reduction and let P be a point of infinite order in $E(K(C))$. Let $\pi : S \to C$ be an elliptic surface attached to E. Consider a divisibility sequence $\{D_{nP}\}_{n\in\mathbb{N}}$.

Theorem 2.1. *Let $K(C)$ be a field of characteristic 0. There exists a constant $N = N(g(C))$ which depends only on the genus of C, such that for all $n \geq N$ the divisor D_{nP} has a primitive valuation.*

Theorem 2.2. *Let $K(C)$ be a field of characteristic 0. There exists a constant $N = N(\chi(S))$ which depends only on the Euler characteristic of surface S, such that for all $n \geq N$ the divisor D_{nP} has a primitive valuation.*

Proofs of both theorems are presented in Section 7.

Now let us assume that $p = \operatorname{char} K(C) \geq 5$. Let p^r be the inseparable degree of the j-map of E if j is nonconstant, otherwise we put 1. Let us assume that the multiplication by p-map has inseparable degree p. We say that E is tame when locally at all places the valuation of the leading term of the formal group homomorphisms $\widehat{[p]}$ is less than p. Otherwise we say that E is wild, cf. Definition 8.3. Both assumptions imply that E is ordinary or in other words that it has ordinary reduction at all places, cf. Section 8.

Theorem 2.3 (Theorem 8.11)**.** *Assume that E is ordinary and tame. There exists an explicit constant $N = N(g(C), p, r)$ which depends only on the genus of C, p and r such that for all $n \geq N$ the divisor D_{nP} has a primitive valuation.*

Theorem 2.4 (Theorem 8.13)**.** *Let E be an elliptic curve defined over $K(C)$ of characteristic $p > 3$ with field of constants $K = \mathbb{F}_q$, $q = p^s$. Let E be ordinary and wild. There exists an explicit constant $N = N(g(C), \chi(S), p, r, s)$ which depends only on the genus of C, Euler characteristic $\chi(S)$, p, r and s such that for all $n \geq N$ the divisor D_{nP} has a primitive valuation.*

When the multiplication by p map is of inseparable degree p^2 we can find examples of curves with infinitely many nonprimitive divisors in the divisibility sequence. They are discussed in Section 9.

3. Notation

- $\chi(S)$ — the Euler characteristic $\chi(S, \mathcal{O}_S)$ of a surface S;
- $g(C)$ — the genus of a curve C;
- $K(C)$ — the function field of a curve C over a field of constants K; the field K will usually be algebraically closed, unless otherwise specified;
- E — an elliptic curve over $K(C)$;
- j — the j-invariant of E;
- Δ_E — the minimal discriminant divisor of E;
- $\widehat{h}_E(P)$ — the canonical height of a point P;
- $h_{K(C)}(E)$ — the height of E defined to be $h_{K(C)}(E) = \frac{1}{12} \deg \Delta_E$;
- $\{D_{nP}\}_{n \in \mathbb{N}}$ — a divisibility sequence attached to a point P.

4. Preliminaries

We will use the notation similar to that in [24]. By

$$\langle \cdot, \cdot \rangle : E(K(C)) \times E(K(C)) \to \mathbb{Q}$$

we denote the symmetric bilinear pairing on $E(K(C))$ which induces the structure of a positive-defined lattice on $E(K(C))/E(K(C))_{\text{tors}}$, cf. [24, Thm. 8.4]. The pairing $\langle \cdot, \cdot \rangle$ induces the height function $P \mapsto \langle P, P \rangle$ which corresponds to the canonical height. For a point $P \in E(K(C))$ we denote by $\overline{P}$ the image of its associated section $\sigma_P : C \to S$ in the given elliptic

surface model. By $C_1.C_2$ we denote the intersection pairing of two curves C_1, C_2 lying on S. We denote by $G(F_v)$ the group of simple components of the fibre $F_v = \pi^{-1}(v)$ above $v \in C$. In Figure 1, following [27, Chap. IV, §9], we present all possible group structures of $G(F_v)$ corresponding to different Kodaira types of singular fibres F_v. We denote by B the set of all places $v \in C$ of bad reduction.

$$\begin{aligned} G(I_n) &\cong \mathbb{Z}/n \\ G(I^*_{2m}) &\cong (\mathbb{Z}/2)^2 \\ G(I^*_{2m+1}) &\cong (\mathbb{Z}/4) \\ G(II) \cong G(II^*) &\cong \{0\} \\ G(III) \cong G(III^*) &\cong \mathbb{Z}/2 \\ G(IV) \cong G(IV^*) &\cong \mathbb{Z}/3 \end{aligned}$$

FIGURE 1. Group of components of fibre with a certain Kodaira type

type of F_v	III	III^*	IV	IV^*	I_b $(b \geq 2)$	I^*_b $(b \geq 0)$
$c_v(P)$, $i = comp_v(P)$	$1/2$	$3/2$	$2/3$	$4/3$	$i(b-i)/b$	$\begin{cases} 1 & (i=1) \\ 1+b/4 & (i>1) \end{cases}$
$c_v(P,Q)$, $i = comp_v(P)$, $j = comp_v(Q)$, $i < j$	–	–	$1/3$	$2/3$	$i(b-j)/b$	$\begin{cases} 1/2 & (i=1) \\ 2+b/4 & (i>1) \end{cases}$

FIGURE 2. Values of correcting terms $c_v(P,Q)$ for all possible singular fibre types with at least two components

By [24, (2.31)] it is possible to write the height pairing in terms of explicit numbers. We denote by $c_v(P,Q)$ the correcting terms that are determined by computation of intersection of curves $\overline{P}$ and $\overline{Q}$ in the fibre above v, cf. Figure 2 reproduced from [24, 8.16]. The values $c_v(P,Q)$ depend on the numbering of components in the fibre above v. For a point P we denote by $comp_v(P)$ the component above v that intersects the curve $\overline{P}$. For a fibre F_v above v we only label the simple components. The unique component that intersects the image of the zero section $\overline{O}$ is denoted by $\Theta_{v,0}$ and we put $comp_v(P) = 0$ if the image $\overline{P}$ intersects $\Theta_{v,0}$. For the fibres of type I_n with $n > 1$ we put labels $\Theta_{v,0}, \Theta_{v,1}, \ldots, \Theta_{v,n-1}$ cyclically, fixing one of two possible choices. For F_v of type I^*_n we denote by $\Theta_{v,1}$ the component which intersects the same double component as $\Theta_{v,0}$. The other two simple components $\Theta_{v,2}$ and $\Theta_{v,3}$ are labelled in an arbitrary way. For the other additive reduction types we choose one fixed labelling (the order is irrelevant).

For two points P and Q we put $c_v(P,Q) = 0$ whenever $comp_v(P) = 0$ or $comp_v(Q) = 0$. The nontrivial cases are described in Figure 2. In [24, Thm. 8.6] it is proved that

$$\langle P, Q\rangle = \chi(S) + \overline{P}.\overline{O} + \overline{Q}.\overline{O} - \overline{P}.\overline{Q} - \sum_{v\in B} c_v(P,Q).$$

In particular we have the equality

$$\langle P, P\rangle = 2\chi(S) + 2\overline{P}.\overline{O} - \sum_{v\in B} c_v(P,P) \tag{4.1}$$

The notion of canonical height from [9, §1] is slightly different from the notion of the height determined by $\langle\cdot,\cdot\rangle$. In fact the first is defined by the limit

$$\widehat{h}_E(P) = \lim_{n\to\infty} \frac{\deg \sigma_{nP}^*\overline{O}}{n^2}.$$

using our notation. By [27, Chap. III Thm. 9.3] the following equality holds

$$\widehat{h}_E(P) = \frac{1}{2}\langle P, P\rangle. \tag{4.2}$$

We also remark that $\deg \sigma_{nP}^*\overline{O} = \deg D_{nP} = \overline{nP}.\overline{O}$ which clearly follows from the definition.

For a fibre above v let us denote by m_v the number of irreducible components in F_v. For the fibre $F_v = \pi^{-1}(v)$ with m_v components the Euler number $e(F_v)$ (cf. [1, Prop. 5.1.6]) equals 0 at v of good reduction, m_v at places v of bad multiplicative reduction and $m_v + 1$ at places of bad additive reduction.

$$e(F_v) = \begin{cases} 0 & v \text{ has good reduction} \\ m_v & v \text{ has multiplicative reduction} \\ m_v + 1 & v \text{ has additive reduction.} \end{cases}$$

By [24, Thm. 2.8] it follows that the square of the canonical bundle K_S^2 is 0 and by Noether's formula [8, Chap. V, Rem. 1.6.1] and [1, Prop. 5.1.6]

$$12\chi(S) = e(S) = \sum_{v\in B}(e(F_v) + \delta_v). \tag{4.3}$$

The terms δ_v are nonnegative and nonzero only in the special cases of $\operatorname{char} K = 2, 3$. We denote by Δ_E the sum $\sum_{v\in C}(\operatorname{ord}_v \Delta_v)\,(v)$ where $\operatorname{ord}_v \Delta_v$ is the order of vanishing of the minimal discriminant Δ_v of E at v. On the other hand by Tate's algorithm [32] $e(F_v)$ equals $\operatorname{ord}_v \Delta_v$ when characteristic p equals 0 or is greater than 3. This implies the equalities

$$h_{K(C)}(E) = \frac{1}{12}\deg \Delta_E = \frac{1}{12}\sum_{v\in C}(\operatorname{ord}_v \Delta_v)\,(v) = \frac{1}{12}e(S) = \chi(S).$$

5. Arithmetic functions

We will use further two arithmetical functions:

$$d(n) = \sum_{m|n} 1,$$
$$\sigma_2(n) = \sum_{m|n} m^2.$$

For the applications in Section 7 it is often enough to use the trivial bound $d(n) \leq n$. However, for the applications in Section 8 a stronger bound [17] is required

$$d(n) \leq n^{1.5379 \log 2/ \log\log n} \quad \text{for } n \geq 3. \tag{5.1}$$

We easily obtain the following estimate

$$\begin{aligned}\sigma_2(n) &= \sum_{m|n} m^2 = n^2 \prod_{p^\alpha || n} (1 + p^{-2} + \ldots + p^{-2\alpha}) \\ &\leq n^2 \prod_{p|n} (1 + p^{-2} + \ldots) = n^2 \prod_{p|n} \left(\frac{1}{1-p^{-2}}\right) \\ &\leq n^2 \prod_{p} \left(\frac{1}{1-p^{-2}}\right) = n^2 \zeta(2) < n^2 \cdot 1.645\end{aligned}$$

It implies that for any $n > 0$ we have

$$\sigma_2(n) < \zeta(2) n^2 < 1.645 n^2. \tag{5.2}$$

For a fixed prime number p we define also functions

$$d^{(p)}(n) = \sum_{m|n} p^{v_p(n/m)},$$
$$\sigma_2^{(p)}(n) = \sum_{m|n} p^{v_p(n/m)} m^2.$$

We denote by $v_p(n)$ the standard p-adic valuation of n at p.

Proposition 5.1. The functions $\sigma_2^{(p)}(n)$ and $d^{(p)}(n)$ are multiplicative and they satisfy:

- $d^{(p)}(n) = \frac{p^{e+1}-1}{(e+1)(p-1)} \cdot d(n)$
- $\sigma_2^{(p)}(n) = \frac{p^e(p+1)}{p^{e+1}+1} \sigma_2(n) < (1 + \frac{1}{p}) \zeta(2) n^2$

where $n = n_0 p^e$, $p \nmid n_0$ and $e = v_p(n)$.

Proof. Put $f(n) = p^{v_p(n)}$. We observe that $d^{(p)}(n)$ is the Dirichlet convolution of $d(n)$ with $f(n)$. Similarly $\sigma_2^{(p)}(n)$ is a convolution of $f(n)$ with $\sigma_2(n)$. The multiplicativity follows and the rest is an easy exercise. □

6. Bounds on the canonical height

In this section we collect together certain lower bounds on canonical height $\widehat{h}_E(P)$ of a point of infinite order. The first presented bound is slightly weaker than the analogue of Lang's conjecture [9] but its proof relies entirely on the theory of Mordell–Weil lattices and the outcome does not depend on the characteristic of the field $K(C)$.

Lemma 6.1. *Assume E is an elliptic curve over $K(C)$. Let P be a point of infinite order in $E(K(C))$. Then*

$$1/\widehat{h}_E(P) \leq 24 \cdot 3^{4\chi(S)}.$$

Proof. If P is a point of infinite order in $E(K(C))$, then the height $\langle P, P\rangle$ is positive. More precisely if we put

$$m = LCM(\{|G(F_v)| : v \in B\})$$

then $\langle P, P\rangle \geq 1/m$ by [24, Lem. 8.3] and [24, Thm. 8.4]. The quantity $1/\langle P, P\rangle$ is bounded from above by $LCM(\{|G(F_v)| : v \in B\})$ and

$$LCM(\{|G(F_v)| : v \in B\}) \leq 12 \prod_{v \in B_{mult,\geq 2}} m_v,$$

where $B_{mult,\geq 2}$ denotes the set of places v of multiplicative reduction and such that $m_v \geq 2$. We take the smallest possible $a \in \mathbb{R}$ such that for all integers $n \geq 2$ we have $n \leq a^n$. It implies that $a = \sup_{n\geq 2} n^{1/n} = 3^{1/3}$. It follows from (4.3) that

$$\prod_{v \in B_{mult,\geq 2}} m_v \leq a^{\sum_{v \in B_{mult,\geq 2}} m_v} \leq 3^{4\chi(S)}.$$

To finish the proof we apply (4.2). □

We define the *conductor* of E to be a divisor $N_E = \sum_{v\in C} u_v\,(v)$ where

$$u_v = \begin{cases} 0 & \text{if the fibre at } v \text{ is smooth,} \\ 1 & \text{if the fibre at } v \text{ is multiplicative,} \\ 2 + \delta_v & \text{if the fibre at } v \text{ is additive,} \end{cases}$$

and the nonnegative numbers δ_v are zero for $\operatorname{char} K(C) \neq 2, 3$. Let $j(E)$ denote the j-invariant of $E/K(C)$ treated as a function. When $j(E)$ is nonconstant then let p^r be its inseparable degree. If $\operatorname{char} K(C) = 0$, then we put 1.

Theorem 6.2 ([19, Thm. 0.1])**.** *Assume E is an elliptic curve over $K(C)$. Let p denote the characteristic of $K(C)$. When the map $j(E)$ is constant or $p = 0$, then*

$$\deg \Delta_E \leq 6(2g(C) - 2 + \deg N_E).$$

When $j(E)$ is nonconstant, $p > 0$ and p^r is its inseparable degree, then

$$\deg \Delta_E \leq 6p^r(2g(C) - 2 + \deg N_E).$$

We denote by σ_E the so-called *Szpiro ratio* which is defined as

$$\sigma_E = \frac{\deg \Delta_E}{\deg N_E}.$$

We denote by $LCM(1,2,\ldots,n)$ the least common multiple of all integers in the interval $[1,n]$.

Theorem 6.3 ([9, Thm. 4.1])**.** *Let E be an elliptic curve over $K(C)$ and let P be a point of infinite order. Let $M \geq 1$, $N \geq 2$ be any integers. Then*

$$\widehat{h}_E(P) \geq \frac{6\left(\left(1+\frac{1}{M}\right)\frac{1}{\sigma_E} - \frac{1}{M} - \frac{1}{N}\right)\cdot h_{K(C)}(E)}{(M+1)(M+2)\,\mathrm{LCM}(1,2,\ldots,N-1)^2}.$$

The following fact is due to Rosser and Schoenfeld [22]. For the proof see [9, Lem. 4.3].

Lemma 6.4. *For all integers $n \geq 1$*

$$\log(\mathrm{LCM}(1,\ldots,n)) < 1.04n.$$

We reproduce the main result of [9] with slightly corrected numerical constants.

Theorem 6.5 ([9, Thm. 6.1])**.** *Let $K(C)$ be a field of characteristic 0. Let P be a nontorsion point in $E(K(C))$. For $h_{K(C)}(E) \geq 2(g(C)-1)$ we have*

$$\widehat{h}_E(P) \geq 10^{-15.5} h_{K(C)}(E).$$

For $h_{K(C)}(E) < 2(g(C)-1)$ we have

$$\widehat{h}_E(P) \geq 10^{-9-23g(C)} h_{K(C)}(E).$$

Proof. From the first assumption and Theorem 6.2 it follows that $\sigma_E \leq 12$. To prove the first inequality we apply Theorem 6.3 with $M = 213$ and $N = 13$.

To prove the second statement we assume that $h_{K(C)}(E) < 2(g(C)-1)$. Value $h_{K(C)}(E)$ is positive, so $g(C) \geq 2$. By assumption our curve has at least one place of bad reduction, hence $\deg N_E \geq 1$. The definition of σ_E implies that

$$\sigma_E \leq 12 h_{K(C)}(E) < 24g(C).$$

Let $M = 601g(C)$ and $N = 25g(C)$. We combine Theorem 6.3 with Lemma 6.4. It follows that

$$\frac{\widehat{h}_E(P)}{h_{K(C)}(E)} \geq \frac{0.0016676e^{-52g(C)}}{g(C)^2(300g(C)+1)(600g(C)+1)} \geq 10^{-9-23g(C)}. \qquad \square$$

We can now proceed in a similar way to obtain the analogue of Lang's conjecture for function fields $K(C)$ of positive characteristic. The bound is worse than in characteristic 0 case, because we have to take into account the inseparable degree of the j-map.

Lemma 6.6. *Let P be a point of infinite order on E over $K(C)$ of positive characteristic p and assume that the j-map of E has inseparable degree p^r. For $h_{K(C)}(E) \geq 2 \cdot p^r(g(C)-1)$ we have*

$$\widehat{h}_E(P) \geq 10^{-18p^r} h_{K(C)}(E).$$

For $h_{K(C)}(E) < 2 \cdot p^r(g(C)-1)$ it follows that

$$\widehat{h}_E(P) \geq 10^{-36g(C)p^r} h_{K(C)}(E).$$

Proof. Under the assumption $h_{K(C)}(E) \geq 2 \cdot p^r(g(C)-1)$ Theorem 6.2 implies that

$$\frac{1}{\sigma_E} \geq \frac{1}{12p^r}.$$

Put $x = p^r$. We choose $M \geq 1$ and $N \geq 2$ such that

$$\left(\left(1+\frac{1}{M}\right)\frac{1}{\sigma_E} - \frac{1}{M} - \frac{1}{N}\right) > 0.$$

We take $M = 200x^2$ and $N = 12x+1$. Lemma 6.4 combined with Theorem 6.3 implies that

$$\widehat{h}_E(P) \geq \phi(x) h_{K(C)}(E)$$

where $\phi(x) = \frac{e^{-24.96x}\left(56x^2+1\right)}{800x^3(12x+1)(100x^2+1)(200x^2+1)}$. For $x \geq 1$ we have the lower bound $\phi(x) \geq 10^{-18x} = 10^{-18p^r}$.

We assume that $h_{K(C)}(E) < 2 \cdot p^r(g(C)-1)$. Definition of σ_E implies that $\sigma_E < 24p^r(g(C)-1) < 12x$ with $x = 2g(C)p^r$. For M and N as before we obtain

$$\widehat{h}_E(P) \geq \phi(x) h_{K(C)}(E)$$

with $\phi(x) \geq 10^{-36g(C)p^r}$. □

Remark 6.7. In positive characteristic and for constant j-map the bound on $\widehat{h}_E(P)$ can be as good as in Theorem 6.5. For $K(C)$ with $\operatorname{char} K(C) = 0$ we can even prove that $\widehat{h}_E(P) \geq \frac{1}{144} h_{K(C)}(E)$, cf. [9, Thm. 6.1]. However, to simplify the statements, we don't make a distinction because the general weaker bounds apply as well.

7. Characteristic 0 argument

Let $\{D_{nP}\}_{n\in\mathbb{N}}$ be an elliptic divisibility sequence attached to a point P in $E(K(C))$ of infinite order. Let v denote a place in $K(C)$. Let $m(v)$ be a positive integer defined as follows

$$m(v) := \min\{n \geq 1 : \operatorname{ord}_v(D_{nP}) \geq 1\}.$$

For a divisor D_{nP} we define a new divisor D_{nP}^{new} by the recipe

$$\operatorname{ord}_v D_{nP}^{\text{new}} = \begin{cases} \operatorname{ord}_v D_{nP}, & m(v) = n, \\ 0, & \text{otherwise.} \end{cases}$$

From this definition it follows by [11, Lem. 5.6] that

$$\begin{aligned} D_{nP} &= \sum_{v\in \operatorname{Supp} D_{nP}} \left(\operatorname{ord}_v D_{nP}\right)(v) \\ &= \sum_{v\in \operatorname{Supp} D_{nP}} \left(\operatorname{ord}_v D_{m(v)P}\right)(v) \quad \text{(from characteristic 0 assumption)} \\ &= \sum_{\substack{v\in \operatorname{Supp} D_{nP} \\ m(v)<n}} \left(\operatorname{ord}_v D_{m(v)P}\right)(v) + \sum_{v\in \operatorname{Supp} D_{nP}^{\text{new}}} \left(\operatorname{ord}_v D_{nP}^{\text{new}}\right)(v) \\ &\leq \sum_{\substack{m|n \\ m<n}} D_{mP} + D_{nP}^{\text{new}}. \end{aligned}$$

It follows that for a divisor D_{nP} which has no primitive valuations, i.e. such that $\operatorname{Supp} D_{nP} \subset \bigcup_{m<n} \operatorname{Supp} D_{mP}$ the following inequality

$$D_{nP} \leq \sum_{\substack{m|n \\ m<n}} D_{mP}$$

holds. We apply the formula of Shioda for the height pairing to make the terms $O(1)$ from the proof of [11, Thm. 5.5] explicit. We rely fundamentally on the following estimate

$$\deg D_{nP} \leq \sum_{\substack{m|n \\ m<n}} \deg D_{mP} \qquad (\Longleftrightarrow) \qquad \overline{nP}.\overline{O} \leq \sum_{\substack{m|n \\ m<n}} \overline{mP}.\overline{O}. \tag{7.1}$$

We define two quantities that will be used frequently

$$\begin{aligned} C_1(n,P) &= \frac{1}{2}\sum_{v\in B} c_v(nP,nP), \\ C_2(n,P) &= \frac{1}{2}\sum_{\substack{m|n \\ m<n}} \sum_{v\in B} c_v(mP,mP). \end{aligned}$$

Assume $n>1$ and D_{nP} is not primitive. We apply formulas (4.1) and (7.1) to obtain the following chain of inequalities and equalities

$$\begin{aligned} n^2\widehat{h}_E(P) &= \widehat{h}_E(nP) = \frac{1}{2}\langle nP, nP\rangle \\ &= \overline{nP}.\overline{O} + \chi(S) - \frac{1}{2}\sum_{v\in B} c_v(nP,nP) \\ &\leq \sum_{\substack{m|n \\ m<n}} \overline{mP}.\overline{O} + \chi(S) - \underbrace{\left(\frac{1}{2}\sum_{v\in B} c_v(nP,nP)\right)}_{C_1(n,P)} \\ &= \sum_{\substack{m|n \\ m<n}} \left(\frac{1}{2}\langle mP,mP\rangle - \chi(S) + \frac{1}{2}\sum_{v\in B} c_v(mP,mP)\right) + \chi(S) - C_1(n,P) \end{aligned}$$

$$= \frac{1}{2}\langle P,P\rangle \sum_{\substack{m|n\\ m<n}} m^2 - \chi(S)\sum_{\substack{m|n\\ m<n}} 1$$
$$+ \underbrace{\frac{1}{2}\sum_{\substack{m|n\\ m<n}}\sum_{v\in B} c_v(mP,mP)}_{C_2(n,P)} + \chi(S) - C_1(n,P)$$
$$= \frac{1}{2}\langle P,P\rangle(\sigma_2(n)-n^2) - \chi(S)(d(n)-2) + C_2(n,P) - C_1(n,P)$$
$$= \widehat{h}_E(P)(\sigma_2(n)-n^2) - \chi(S)(d(n)-2) + C_2(n,P) - C_1(n,P).$$

This can be rewritten in the following form

$$\chi(S)(d(n)-2)+C_1(n,P)+n^2\widehat{h}_E(P) \le \widehat{h}_E(P)(\sigma_2(n)-n^2)+C_2(n,P). \tag{7.2}$$

Lemma 7.1. *Let P be a point of infinite order in $E(K(C))$ and let $n>1$ and assume D_{nP} is not primitive. Then*

$$n^2\widehat{h}_E(P) \le \widehat{h}_E(P)(\sigma_2(n)-n^2) + C_2(n,P). \tag{7.3}$$

Proof. Since $n>1$ it is always true that $d(n)\ge 2$, the factor $\chi(S)$ is always positive and the terms in $C_1(n,P)$ are also non-negative by their definition. It implies that we can drop first two terms of the inequality (7.2). □

Let $E(K(C))^0$ denote the subgroup of $E(K(C))$ such that for each $P\in E(K(C))^0$ the curve $\overline{P}$ intersects the same component as the curve $\overline{O}$ in every fibre of $\pi: S\to C$. For such points we always have $c_v(P,P)=0$.

Corollary 7.2. *With the notation from the previous lemma if P lies in $E(K(C))^0$, then every divisor D_{nP} is primitive.*

Proof. We use the inequality (7.3) and apply the assumption $C_2(n,P)=0$. It follows by (5.2) that

$$n^2\widehat{h}_E(P) \le \widehat{h}_E(P)(\zeta(2)-1)n^2.$$

We can divide by $\widehat{h}_E(P)$ because P is a point of infinite order, hence

$$2n^2 \le \zeta(2)n^2$$

and $n=0$. □

Lemma 7.3. *Let $K(C)$ be a field of characteristic $p\neq 2,3$. For a point $P\in E(K(C))$ and any $k\in\mathbb{Z}$ we have*

$$\sum_{v\in B} c_v(kP,kP) \le 3\chi(S).$$

Proof. We denote by B_{mult} the set of points v in $C(K)$ such that F_v has multiplicative reduction. We denote by $B_{add,1}$ the set of points with additive reduction of type I_n^* and by $B_{add,III}$, B_{add,III^*}, $B_{add,IV}$ and B_{add,IV^*} the sets of points with respectively reduction of type III, III^*, IV and IV^*. Let

$B_{add,2}$ denote the set of all places of bad additive reduction not contained in $B_{add,1}$. Let $v \in B_{mult}$, then it follows from Figure 2 that

$$c_v(kP, kP) \leq \frac{i(m_v - i)}{m_v}$$

for certain i. The function on the right-hand side is quadratic with respect to i and reaches the maximum at $m_v/2$, hence $c_v(kP, kP) \leq \frac{m_v}{4}$. That inequality and other values in Figure 2 allow us to give the upper bounds

$$\sum_{v \in B_{mult}} c_v(kP, kP) \leq \frac{1}{4} \sum_{v \in B_{mult}} m_v$$

$$\sum_{v \in B_{add,III}} c_v(kP, kP) \leq \frac{1}{2} |B_{add,III}|$$

$$\sum_{v \in B_{add,III^*}} c_v(kP, kP) \leq \frac{3}{2} |B_{add,III^*}|$$

$$\sum_{v \in B_{add,IV}} c_v(kP, kP) \leq \frac{2}{3} |B_{add,IV}|$$

$$\sum_{v \in B_{add,IV^*}} c_v(kP, kP) \leq \frac{4}{3} |B_{add,IV^*}|.$$

For points v of type $B_{add,1}$ we have $c_v(kP, kP) \leq \frac{m_v - 1}{4} = \frac{m_v + 1}{4} - \frac{1}{2}$. This leads to

$$2 \cdot |B_{add,1}| + 4 \sum_{v \in B_{add,1}} c_v(kP, kP) \leq \sum_{v \in B_{add,1}} (m_v + 1).$$

It follows from (4.3) that

$$12\chi(S) = \sum_{v \in B} e(F_v) = \sum_{v \in B_{mult}} m_v + \sum_{v \in B_{add,1}} (m_v + 1) + \sum_{v \in B_{add,2}} (m_v + 1).$$

But we also have

$$\sum_{v \in B_{add,2}} (m_v + 1) = 3 \cdot |B_{add,III}| + 9 \cdot |B_{add,III^*}| + 4 \cdot |B_{add,IV}| + 8 \cdot |B_{add,IV^*}|$$

by [27, Chap. IV, Table 4.1]. It follows that

$$12\chi(S) \geq 4 \sum_{v \in B_{mult}} c_v(kP, kP) + 4 \sum_{v \in B_{add,1}} c_v(kP, kP) + 6 \sum_{v \in B_{add,2}} c_v(kP, kP)$$

which is even stronger than what we wanted to prove. □

Remark 7.4. The statement of Lemma 7.3 is equivalent to [2, Lem. 3]. The upper bound in loc. cit. follows from (4.1).

Lemma 7.5. *Let $K(C)$ be a field of characteristic 0. Let P be a point in $E(K(C))$. Then*

$$C_2(n, P) \leq \frac{3}{2} \chi(S)(d(n) - 1).$$

Proof. This follows simply from the definition of $C_2(n,P)$ and Lemma 7.3. □

Corollary 7.6. *Let P be a point of infinite order in $E(K(C))$. Suppose that D_{nP} is not primitive, then*

$$n^2 \leq \frac{36 \cdot \chi(S) \cdot 3^{4\chi(S)}}{(2-\zeta(2))} d(n).$$

Proof. Combine Lemmas 6.1, 7.1 and 7.5. □

Corollary 7.7. *Let $K(C)$ be a field of characteristic 0. Let P be a point of infinite order in $E(K(C))$. If D_{nP} is not primitive, then*

$$n^2 \leq \frac{1.5 \cdot 10^9}{(2-\zeta(2))} d(n) \cdot \begin{cases} 10^{6.5}, & \chi(S) \geq 2(g(C)-1), \\ 10^{23g(C)}, & \chi(S) < 2(g(C)-1). \end{cases}$$

Proof. To bound the quantity $1/\widehat{h}_E(P)$ we apply Theorem 6.5. Suppose that $\chi(S) \geq 2(g(C)-1)$, then

$$1/\widehat{h}_E(P) \leq 10^{15.5} \cdot 1/\chi(S).$$

Combining this with the argument in Lemma 7.5 we obtain

$$1/\widehat{h}_E(P) \cdot C_2(n,P) \leq 10^{15.5} \cdot 1/\chi(S) \cdot 1.5 \cdot \chi(S) \cdot d(n) = 1.5 \cdot 10^{15.5} d(n).$$

It follows that

$$n^2 \leq (1.5 \cdot 10^{15.5})/(2-\zeta(2)) \cdot d(n). \tag{7.4}$$

On the contrary, when $\chi(S) < 2(g(C)-1)$ we get

$$1/\widehat{h}_E(P) \cdot C_2(n,P) \leq 10^{9+23g(C)} \cdot 1/\chi(S) \cdot 1.5 \cdot \chi(S) \cdot d(n) = 1.5 \cdot 10^{9+23g(C)} d(n).$$

Similarly, we get

$$n^2 \leq (1.5 \cdot 10^{9+23g(C)})/(2-\zeta(2)) \cdot d(n). \tag{7.5}$$

The corollary follows from those two estimates. □

Proof of Theorem 2.1. We have the trivial estimate $d(n) \leq n$. Corollary 7.7 implies that

$$n^2 \leq Cn$$

for a constant C that depends only on $g(C)$. So $n \leq C$ and the theorem follows. □

Proof of Theorem 2.2. There exists a constant C that depends only on $\chi(S)$ as in Corollary 7.6 such that $n^2 \leq Cn$. □

Remark 7.8. If we assume that $n \geq N_0$ where N_0 is sufficiently large, we obtain due to (5.1) a much better bound for $d(n)$. This will lead in practice to a much smaller bound for the number of nonprimitive divisors.

8. Characteristic p argument

Let v be a discrete valuation on $K(C)$. It determines the completion $K(C)_v$ of the field $K(C)$ with respect to v with ring of integers R_v and maximal ideal $\mathcal{M}_v$. We consider below only fields $K(C)$ of characteristic at least 5. For an elliptic curve E over $K(C)$ we consider its minimal Weierstrass model $E^{(v)}$ at v, cf. [25, Chap. VII, §1]. Such a model is unique up to an admissible change of coordinates, cf. [25, Chap. VII, Prop. 1.3]. We denote by $\widehat{E}^{(v)}$the formal group attached to the minimal Weierstrass equation $E^{(v)}$ in the sense of [25, Chap. IV]. Multiplication by p map gives rise to a homomorphism of formal groups $\widehat{[p]}_v : \widehat{E}^{(v)} \to \widehat{E}^{(v)}$. Its height h equals 1 or 2, cf.[25, Chap. IV, Thm. 7.4]. If the height equals h, then $\widehat{[p]}_v(T) = g(T^{p^h})$ where $g(T) \in R_v[[T]]$ and $g'(0) \neq 0$. The coefficient of T^p in $\widehat{[p]}_v(T)$ is denoted by $H(E, v)$ and is the Hasse invariant in the sense of [14, 12.4]. The valuation $h_{E,v} := \operatorname{ord}_v(H(E, v))$ does not depend of the minimal model at v by [13, Ka-29]. We say that the curve E is *ordinary* when for all discrete valuations v of $K(C)$ the homomorphism $\widehat{[p]}_v$ has height 1.

Lemma 8.1. *Let E over $K(C)$ of characteristic $p > 3$ be an ordinary elliptic curve and let $\chi(S)$ denote the Euler characteristic of the attached elliptic surface $\pi : S \to C$. Then*

$$(p-1)\chi(S) = \sum_{v \in C} h_{E,v}.$$

Proof. For any place v in $K(C)$ we fix a minimal model $E^{(v)}$ of E at v with Hasse invariant $H(E, v)$. Let $\Delta \in K(C)$ be the discriminant and let $H(E) \in K(C)$ denote the Hasse invariant of one arbitrarily chosen model $E^{(v_0)}$ at v_0. We denote by Δ_v the minimal discriminant of E at v. For each v there exists an integer n_v such that

$$\operatorname{ord}_v(\Delta) = \operatorname{ord}_v(\Delta_v) + 12n_v. \tag{8.1}$$

From [13, Ka-29] it follows that

$$\operatorname{ord}_v(H(E)) = \operatorname{ord}_v(H(E, v)) + (p-1)n_v. \tag{8.2}$$

Elements Δ and $H(E)$ correspond to functions $\Delta, H(E) : C \to \mathbb{P}^1$ and hence $\sum_{v \in C} \operatorname{ord}_v(H(E)) = \sum_{v \in C} \operatorname{ord}_v(\Delta) = 0$. Summation over all v combined with (8.1) and (8.2) implies that

$$\frac{(p-1)\sum_{v \in C} \operatorname{ord}_v \Delta_v}{12} = \sum_{v \in C} h_{E,v}.$$

To finish the proof we apply $12\chi(S) = \sum_{v \in C} e(F_v) = \sum_{v \in C} \operatorname{ord}_v \Delta_v$. □

We generalise [11, Lemma 5.6] to the case of positive characteristic. We note that a similar lemma can be obtained in the number field case, cf. [30].

Lemma 8.2. *Let E be an ordinary elliptic curve over $K(C)$, field of characteristic p. Let $\{D_{nP}\}_{n\in\mathbb{N}}$ be an elliptic divisibility sequence attached to a point P in $E(K(C))$ of infinite order. Let v denote a place in $K(C)$. Let $m(v)$ be a positive integer defined as follows*

$$m(v) := \min\{n \geq 1 : \operatorname{ord}_v(D_{nP}) \geq 1\}.$$

If $h_{E,v} \leq p-1$, then for all $n \geq 1$ the following equality

$$\operatorname{ord}_v D_{nP} = \begin{cases} p^e \operatorname{ord}_v D_{m(v)P} + \frac{p^e-1}{p-1} h_{E,v}, & m(v) \mid n, \\ 0, & m(v) \nmid n, \end{cases}$$

holds for $e = v_p(\frac{n}{m(v)})$.

Let $k \geq \lceil \log_p(\frac{p+(p-1)^2\chi(S)}{2p-1}) \rceil$ be an integer. For $h_{E,v} \geq p$ and for all $n \geq 1$ the following equality

$$\operatorname{ord}_v D_{nP} = \begin{cases} p^e \operatorname{ord}_v D_{m(v)P} + \delta(e), & m(v) \mid n,\ e \leq k, \\ p^e \operatorname{ord}_v D_{m(v)P} + \frac{p^{e-k}-1}{p-1} h_{E,v} + p^{e-k}\delta(k), & m(v) \mid n,\ e > k, \\ 0, & m(v) \nmid n, \end{cases}$$

holds for $e = v_p(\frac{n}{m(v)})$. Function $\delta(e)$ depends on P and v and satisfies the estimates for $e \geq 1$

$$p \cdot \frac{p^e-1}{p-1} \leq \delta(e) \leq p^{2e} m(v)^2 \widehat{h}_E(P) + \frac{1}{2}\chi(S) - p^e.$$

Proof. Let $E(K(C))_{v,r}$ denote the set

$$\{P \in E(K(C)) : \operatorname{ord}_v \sigma_P^* \overline{O} \geq r\} \cup \{\mathcal{O}\}.$$

It follows from its definition that $E(K(C))_{v,r}$ is a subgroup of $E(K(C))$. Number $\operatorname{ord}_v D_{nP}$ equals $\max\{r \geq 0 : nP \in E(K(C))_{v,r}\}$. We consider the completion $K(C)_v$ of field $K(C)$ with respect to v, with integer ring $\mathcal{R}_v$ and maximal ideal $\mathcal{M}_v$. Suppose that $d_0 := \operatorname{ord}_v D_{m(v)P}$ and $d := \operatorname{ord}_v D_{nP} \geq 1$. The subgroups $\{E(K(C))_{v,r}\}_{r\geq 1}$ form a nested sequence so

$$\operatorname{GCD}(m(v), n)P \in E(K(C))_{v,\min\{d_0,d\}}.$$

Minimality of $m(v)$ implies that $m(v) \leq \operatorname{GCD}(m(v), n)$, hence $m(v) \mid n$.

By [25, Chap.VII, Prop. 2.2] there exists an isomorphism

$$i_v : E_1(K(C)_v) \to \widehat{E}(\mathcal{M}_v)$$

given by $(x, y) \to -x/y$ and where $E_1(K(C)_v)$ is the kernel of reduction at v defined in [25, Chap.VII]. We note that the group $E(K(C))_{v,1}$ is a subgroup of $E_{1,v}(K(C)_v)$. For an integer n coprime to p and $P \in E(K(C))_{v,1}$ we have

$$\operatorname{ord}_v(i_v(nP)) = \operatorname{ord}_v(i_v(P)).$$

Assume that $\operatorname{ord}_v(h_{E,v}) \leq p-1$. It follows that

$$\operatorname{ord}_v(i_v(pP)) = h_{E,v} + p \operatorname{ord}(i_v(P)).$$

By iteration we obtain

$$\operatorname{ord}_v(i_v(nP)) = p^e \operatorname{ord}_v(i_v(P)) + h_{E,v}(1 + \ldots + p^{e-1})$$

where $e = v_p(n)$.

For $\operatorname{ord}_v(h_{E,v}) \geq p$ and for any $P \in E(K(C))_{v,1}$ we have

$$\operatorname{ord}_v(i_v(pP)) \geq p + p \operatorname{ord}(i_v(P)).$$

After e iterations this implies that

$$\operatorname{ord}_v(i_v(p^e P)) \geq p \cdot \frac{p^e - 1}{p - 1} + p^e \operatorname{ord}(i_v(P)).$$

The formal group homomorphism $\widehat{[p]}_v$ satisfies

$$\operatorname{ord}_v(\widehat{[p]}_v(T)) = h_{E,v} + p \operatorname{ord}_v(T)$$

for T such that $\operatorname{ord}_v(T) > h_{E,v}$. Lemma 8.1 implies that $h_{E,v} \leq (p-1)\chi(S)$. If e is greater than k, then we have

$$p^e + \frac{p^e - 1}{p - 1} \cdot p > (p-1)\chi(S).$$

Thus $\operatorname{ord}_v i_v(p^e P) = p^e \operatorname{ord}_v(i_v(P)) + h_{E,v}(1 + \ldots + p^{e-k-1}) + \delta(k)$ where $\delta(k) = \operatorname{ord}_v i_v(p^k P) - p^k \operatorname{ord}_v i_v(P)$.

For any $e \leq k$ we define $\delta(e) = \operatorname{ord}_v i_v(p^e P) - p^e \operatorname{ord}_v i_v(P)$. It is clear that $\delta(e) \geq p \cdot \frac{p^e - 1}{p-1}$. For the upper bound we observe that

$$p^{2e} m(v)^2 \widehat{h}_E(P) + \frac{1}{2}\chi(S) \geq \operatorname{ord}_v D_{p^e m(v) P} = \operatorname{ord}_v D_{nP}$$

by property (4.1) and Lemma 7.3. Since $\operatorname{ord}_v D_{m(v)P} \geq 1$, the upper bound follows by replacing P by $m(v)P$ in the definition of $\delta(e)$. □

Definition 8.3. Let E be an ordinary elliptic curve over a function field $K(C)$ of prime characteristic p. We say that E is *tame*, when for all places v we have $h_{E,v} \leq p - 1$. Otherwise we say that E is *wild*.

If $\operatorname{char} K(C) = p > 0$ we apply Lemma 8.2 instead of [11, Lemma 5.6]. Under assumption that D_{nP} has no primitive valuations it follows that

$$\begin{aligned} D_{nP} &= \sum_{v \in \operatorname{Supp} D_{nP}} (\operatorname{ord}_v D_{nP})(v) \\ &= \sum_{\substack{v \in \operatorname{Supp} D_{nP} \\ m(v) < n}} (\operatorname{ord}_v D_{nP})(v) + \sum_{v \in \operatorname{Supp} D_{nP}^{\text{new}}} (\operatorname{ord}_v D_{nP}^{\text{new}})(v) \\ &= \sum_{\substack{v \in \operatorname{Supp} D_{nP} \\ m(v) < n}} (\operatorname{ord}_v D_{nP})(v) \quad \text{(no primitive valuations)} \end{aligned}$$

$$
\begin{aligned}
&= \sum_{\substack{v\in \operatorname{Supp} D_{nP}\\ m(v)<n}} \left(p^{v_p\left(\frac{n}{m(v)}\right)} \operatorname{ord}_v D_{m(v)P}\right)(v) + \underbrace{\sum_{\substack{v\in \operatorname{Supp} D_{nP}\\ m(v)<n}} f(E,P,n,v)\,(v)}_{W(E,P,n)}\\
&\le \sum_{\substack{m|n\\ m<n}} \sum_{v\in C} \left(p^{v_p\left(\frac{n}{m}\right)} \operatorname{ord}_v D_{mP}\right)(v) + W(E,P,n)\\
&= \sum_{\substack{m|n\\ m<n}} p^{v_p\left(\frac{n}{m}\right)} D_{mP} + W(E,P,n).
\end{aligned}
$$

Function $f(E,P,n,v)$ is defined as the difference

$$f(E,P,n,v) = \operatorname{ord}_v D_{nP} - p^{v_p\left(\frac{n}{m(v)}\right)} \operatorname{ord}_v D_{m(v)P}.$$

We can summarize the computations above in the following corollary.

Corollary 8.4. *Let $p>3$ be a prime number. Let E be an ordinary elliptic curve over $K(C)$ and let P be a point of infinite order on E. Assume n is such that D_{nP} is a divisor without primitive valuations. When $p\nmid n$, then*

$$D_{nP} \le \sum_{\substack{m|n\\ m<n}} D_{mP}.$$

When $\operatorname{char} K(C) = p$, *$p \mid n$, $n = n_0 p^e$ and $p\nmid n_0$, then*

$$D_{nP} \le \sum_{\substack{m|n\\ m<n}} p^{v_p\left(\frac{n}{m}\right)} D_{mP} + W(E,P,n). \tag{8.3}$$

We apply the degree function to (8.3). If n is such that D_{nP} has no primitive divisors and $p \mid n$ ($p>3$), then

$$\overline{nP}.\overline{O} \le \sum_{\substack{m|n\\ m<n}} p^{v_p\left(\frac{n}{m}\right)} \overline{mP}.\overline{O} + \deg W(E,P,n).$$

Now we redo the computations from characteristic 0

$$
\begin{aligned}
&n^2 \widehat{h}_E(P)\\
&= \widehat{h}_E(nP) = \frac{1}{2}\langle nP, nP\rangle\\
&= \overline{nP}.\overline{O} + \chi(S) - \frac{1}{2}\sum_{v\in B} c_v(nP,nP)\\
&\le \sum_{\substack{m|n\\ m<n}} p^{v_p\left(\frac{n}{m}\right)} \overline{mP}.\overline{O} + \underbrace{\deg W(E,P,n)}_{C_3(n,p,P)} + \chi(S) - \underbrace{\left(\frac{1}{2}\sum_{v\in B} c_v(nP,nP)\right)}_{C_1(n,P)}
\end{aligned}
$$

$$
\begin{aligned}
&= \sum_{\substack{m|n\\ m<n}} p^{v_p(\frac{n}{m})} \left(\frac{1}{2} \langle mP, mP\rangle - \chi(S) + \frac{1}{2} \sum_{v\in B} c_v(mP, mP) \right) \\
&\quad + C_3(n,p,P) + \chi(S) - C_1(n,P) \\
&= \frac{1}{2} \langle P, P\rangle \sum_{\substack{m|n\\ m<n}} p^{v_p(\frac{n}{m})} m^2 - \chi(S) \sum_{\substack{m|n\\ m<n}} p^{v_p(\frac{n}{m})} \\
&\quad + \underbrace{\frac{1}{2} \sum_{\substack{m|n\\ m<n}} p^{v_p(\frac{n}{m})} \sum_{v\in B} c_v(mP, mP)}_{C_2(n,p,P)} + C_3(n,p,P) + \chi(S) - C_1(n,P) \\
&= \widehat{h}_E(P)(\sigma_2^{(p)}(n) - n^2) - \chi(S)(d^{(p)}(n) - 2) + C_2(n,p,P) \\
&\quad + C_3(n,p,P) - C_1(n,P).
\end{aligned}
$$

Lemma 8.5. *Let $p > 3$ be a prime and let* $\operatorname{char} K(C) = p$. *Let P be a point of infinite order in $E(K(C))$ and let $n > 1$ and assume D_{nP} is not primitive. When $p \nmid n$ then*

$$n^2 \widehat{h}_E(P) \le \widehat{h}_E(P)(\sigma_2(n) - n^2) + C_2(n,P).$$

When $p \mid n$ then

$$n^2 \widehat{h}_E(P) \le \widehat{h}_E(P)(\sigma_2^{(p)}(n) - n^2) + C_2(n,p,P) + C_3(n,p,P).$$

Proof. For n coprime with p Lemma 8.2 implies that our inequalities reduce to the situation known from characteristic 0. Assume now that $p \mid n$. Since $n > 1$ it is always true that $d^{(p)}(n) \ge 2$, the factor $\chi(S)$ is always positive and the terms in $C_1(n,p,P)$ are also non-negative by their definition and the lemma follows. □

We need to establish some crude estimates of $C_2(n,p,P)$ and $C_3(n,p,P)$.

Lemma 8.6. *Let $p > 3$ be a prime and let* $\operatorname{char} K(C) = p$. *Let P be a point of infinite order in $E(K(C))$ and let $n > 1$ and assume D_{nP} is not primitive. We obtain the estimate*

$$C_2(n,p,P) \le \frac{3}{2} \chi(S) \cdot (d^{(p)}(n) - 1). \tag{8.4}$$

Proof. We apply Lemma 7.3 to prove the inequality (8.4). □

To get a uniform result we have to estimate the sum $W(E,P,n)$ independently of n. To achieve this we prove a technical lemma.

Lemma 8.7. *Let E and P be given. Let v denote a place in $K(C)$ and assume $h_{E,v} > 0$.*

Then one of the following cases holds:

- *E at v has good reduction and then $p \nmid m(v)$.*
- *E at v has additive reduction and then $m(v) \mid 12p$.*

- *E at v has multiplicative reduction and $h_{E,v} > 0$ cannot both occur.*

Proof. Assume first that E has good reduction at v. The assumption $h_{E,v} > 0$ implies that locally at v the fibre E_v satisfies $E_v[p] = 0$ by [25, Chap.V, Thm. 3.1]. If $p \mid m(v)$, then $(m(v)/p)P$ would already meet the zero section at v contradicting the minimality of $m(v)$.

If v is of additive reduction, then from Kodaira classification of bad fibres, cf. [27, Chap. IV, Table 4.1] it follows that there exists an integer $k \in \{1, 2, 3, 4\}$ such that the point kP hits the component of zero at v. Either kP is zero locally at v or pkP is zero. It implies that $m(v) \mid 12p$.

Let t be a formal variable and consider the series with coefficients in $\mathbb{Z}[[t]]$ as in [33]

$$b_2(t) = 5\sum_{n=1}^{\infty} \frac{n^3 t^n}{1-t^n} = 5t + 45t^2 + 140t^3 + \cdots$$

$$b_3(t) = \sum_{n=1}^{\infty} \left(\frac{7n^5 + 5n^3}{12}\right) \frac{t^n}{1-t^n} = t + 23t^2 + 154t^3 + \cdots$$

$$\Delta(t) = b_3 + b_2^2 + 72b_2b_3 - 432b_3^2 + 64b_2^3 = t\prod_{n=1}^{\infty}(1-t^n)^{24}$$

$$j(t) = \frac{(1+48b_2)^3}{\Delta} = \frac{1}{t}(1 + 744t + 196884t^2 + \cdots)$$

Finally, let E at v have multiplicative reduction. The normalised v-adic norm of $j(E)$ is greater than 1. There exists a parameter $q \in \mathcal{M}_v$ such that $j(E) = j(q)$ ([21, §3, VII]) and the curve

$$E_q : y^2 + xy = x^3 - b_2(q)x + b_3(q)$$

has j-invariant equal to $j(q)$, has discriminant $\Delta(q)$ and is an elliptic curve over $K(C)_v$. It follows that

$$c_4(E_q) = 1 + 240\sum_{n=1}^{\infty} q^n \sum_{m|n} m^3,$$

$$c_6(E_q) = -1 + 504\sum_{n=1}^{\infty} q^n \sum_{m|n} m^5.$$

It implies that the Weierstrass model E_q is minimal at v and the curves E and E_q are isomorphic over some extension L of $K(C)_v$. The isomorphism corresponds to a change of coordinates between a minimal Weierstrass model of E (with coordinates x' and y') and E_q with $x \mapsto u^2x' + r$, $y \mapsto u^3y' + u^2sx' + t$ where u, s, t belong to the ring of integers of L. We have also $\mathrm{ord}_v(u) = 0$ so the equality $h_{E_q,v} = h_{E,v}$ holds by [13, Ka-29]. By [14, Thm. 12.4.2] we have $h_{E_q,v} = 0$, which contradicts our assumption $h_{E,v} > 0$. □

For the next two lemmas assume that E is an ordinary elliptic curve over $K(C)$, field of characteristic $p > 3$. Let $\{D_{nP}\}_{n\in\mathbb{N}}$ be an elliptic divisibility sequence attached to a point P in $E(K(C))$ of infinite order and let $S \to C$ be an elliptic surface corresponding to E. We denote by e the p-valuation $v_p(n)$ of n.

Lemma 8.8. *Let E be tame. Then*

$$\deg W(E,P,n) \le (p^e - 1)\chi(S).$$

Proof. In the tame situation we have $f(E,P,n,v) \le \frac{p^e-1}{p-1}h_{E,v}$. Combination of this equality with Lemma 8.1 proves the statement. □

Let $\mathcal{R} = \mathcal{R}(P,n) = \{v : v \in \operatorname{Supp} D_{nP},\ m(v) < n\}$. Denote by Σ_g and Σ_a the set of places of respectively good and bad additive reduction of E. Let $\mathcal{R}_g = \mathcal{R} \cap \Sigma_g$ and $\mathcal{R}_a = \mathcal{R} \cap \Sigma_a$. Let $\mathcal{S}$ denote the set of places v in $K(C)$ such that $h_{E,v} > 0$. Let $\Sigma_g^s = \Sigma_g \cap \mathcal{S}$ and $\Sigma_a^s = \Sigma_a \cap \mathcal{S}$.

Lemma 8.9. *Let E be wild and let M denote $\max\{144p^2, \max_{v\in\mathcal{R}_g\cap\mathcal{S}} m(v)^2\}$. The following estimates hold for any n and P of infinite order*

(i) *For $v_p(n) \le \lceil \log_p(\frac{p+(p-1)^2\chi(S)}{2p-1})\rceil$ we have*

$$\deg W(E,P,n) \le (p^e - 1)\chi(S) + \chi(S)p^{2e}\widehat{h}_E(P)M + \frac{1}{2}\chi(S)^2.$$

(ii) *For $v_p(n) > \lceil \log_p(\frac{p+(p-1)^2\chi(S)}{2p-1})\rceil$ we have*

$$\deg W(E,P,n) \le \chi(S)\left((p^e - 1) + p^{e-k}(1 + (p^{2k}M\widehat{h}_E(P) + \frac{1}{2}\chi(S)))\right).$$

Proof. From Lemma 8.2 we can split the expression $\deg W(E,P,n)$ into two parts and estimate them separately.

$$\begin{aligned}\deg W(E,P,n) &= \sum_{v\in\mathcal{R}\cap\mathcal{S}} f(E,P,n,v)\\ &= \sum_{h_{E,v}<p} f(E,P,n,v) + \sum_{h_{E,v}\ge p} f(E,P,n,v)\\ &\le (p^e - 1)\chi(S) + \sum_{h_{E,v}\ge p} f(E,P,n,v).\end{aligned}$$

The last inequality follows from $f(E,P,n,v) \le \frac{p^e-1}{p-1}h_{E,v}$ for $h_{E,v} < p$ and Lemma 8.1. Put $k = \lceil \log_p(\frac{p+(p-1)^2\chi(S)}{2p-1})\rceil$ and assume that $e = v_p(n) \le k$. It follows that

$$f(E,P,n,v) \le p^{2e}m(v)^2\widehat{h}_E(P) + \frac{1}{2}\chi(S) - p^e$$

for v such that $h_{E,v} \ge p$. By Lemma 8.1 there is at most $\frac{p-1}{p}\chi(S)$ such different places v. By Lemma 8.7 they can be only of good or additive

reduction. Hence

$$\sum_{h_{E,v}\geq p} f(E,P,n,v) \leq \frac{p-1}{p}\chi(S)p^{2e}\widehat{h}_E(P)(\max\{\max_{v\in\Sigma_a^s} m(v)^2, \max_{v\in\mathcal{R}_g\cap\mathcal{S}} m(v)^2\}) + \frac{p-1}{p}\chi(S)(\frac{1}{2}\chi(S)-p^e).$$

By Lemma 8.7 it follows that $\max_{v\in\Sigma_a^s} m(v) \leq 12p$, hence

$$\sum_{h_{E,v}\geq p} f(E,P,n,v) \leq \chi(S)p^{2e}\widehat{h}_E(P)M + \frac{1}{2}\chi(S)^2.$$

Assume now that $e > k$. We have the inequality

$$f(E,P,n,v) \leq \frac{p^{e-k}-1}{p-1}h_{E,v} + p^{e-k}\delta(k)$$

where $\delta(k) \leq p^{2k}m(v)^2\widehat{h}_E(P) + \frac{1}{2}\chi(S) - p^k$. It implies that

$$\sum_{h_{E,v}\geq p} f(E,P,n,v)$$
$$\leq (p^{e-k}-1)\chi(S) + \frac{p-1}{p}\chi(S)p^{e-k}\left(p^{2k}M\widehat{h}_E(P) + \frac{1}{2}\chi(S) - p^k\right)$$

or in simplified form

$$\sum_{h_{E,v}\geq p} f(E,P,n,v) \leq p^{e-k}\chi(S) + p^{e-k}\chi(S)\left(p^{2k}M\widehat{h}_E(P) + \frac{1}{2}\chi(S)\right). \quad \square$$

Remark 8.10. We observe that the bound $\lceil \log_p(\frac{p+(p-1)^2\chi(S)}{2p-1})\rceil$ approaches 1 as $p\to\infty$ independently of $\chi(S)$.

Theorem 8.11. *Let E be an elliptic curve over $K(C)$ of positive characteristic $p>3$ with at least one bad fibre. Assume that E is tame. Let $\pi: S\to C$ be the attached elliptic fibration. Let P be a point of infinite order on E. Let p^r be the inseparable degree of the j-map of E. There exists an explicit constant $N = N(g(C),p,r)$ which depends only on the genus of C, p and r such that for all $n\geq N$ the divisor D_{nP} has a primitive valuation.*

Proof. Let n be an integer such that the divisor D_{nP} has no primitive valuation. Let us first assume that $p\nmid n$. Lemma 8.5 implies that

$$n^2\widehat{h}_E(P) \leq \widehat{h}_E(P)(\sigma_2(n)-n^2) + C_2(n,P).$$

We combine the estimate $\sigma_2(n) < \zeta(2)n^2$ with the estimate from Lemma 7.5. The only difference with characteristic zero case is that we apply now the height estimate for $\widehat{h}_E(P)$ from Lemma 6.6. It follows that there exists an effective constant $N_1 = N_1(g(C),p^r)$ such that $n\leq N_1$.

Let us assume that $p\mid n$. After Lemma 8.5 we have

$$n^2\widehat{h}_E(P) \leq \widehat{h}_E(P)(\sigma_2^{(p)}(n)-n^2) + C_2(n,p,P) + C_3(n,p,P).$$

By Proposition 5.1 it follows that

$$n^2\widehat{h}_E(P) \le \widehat{h}_E(P)\cdot\left(\left(1+\frac{1}{p}\right)\zeta(2)-1\right)n^2 + C_2(n,p,P) + C_3(n,p,P)$$

and in simplified form

$$\theta(p)n^2\widehat{h}_E(P) \le C_2(n,p,P) + C_3(n,p,P)$$

where by $\theta(p)$ we denote $2-\left(1+\frac{1}{p}\right)\zeta(2)$. We apply Lemma 8.6 and get the bound

$$\theta(p)n^2\widehat{h}_E(P) \le \frac{3}{2}\chi(S)\cdot(d^{(p)}(n)-1) + \deg W(E,P,n).$$

Put $e = v_p(n)$. Lemma 8.8 implies that $\deg W(E,P,n) \le (p^e-1)\chi(S)$, hence

$$\theta(p)n^2\widehat{h}_E(P) \le \frac{3}{2}\chi(S)\cdot(d^{(p)}(n)-1) + (p^e-1)\chi(S)$$

and again by Proposition 5.1 it follows that

$$\theta(p)n^2\widehat{h}_E(P) \le \frac{3}{2}\chi(S)\cdot\left(\frac{p^{e+1}-1}{(e+1)(p-1)}\cdot d(n)-1\right) + (p^e-1)\chi(S).$$

We rearrange the sum and drop several terms to get

$$\theta(p)n^2\widehat{h}_E(P) \le \left(\frac{3}{2}pd(n)+1\right)p^e\chi(S).$$

For $\chi(S) = h_{K(C)}(E) \ge 2\cdot p^r(g(C)-1)$ the inequality

$$\frac{\chi(S)}{\widehat{h}_E(P)} \le 10^{18p^r}$$

holds. Hence

$$\theta(p)n^2 \le \left(\frac{3}{2}pd(n)+1\right)p^e\cdot 10^{18p^r}.$$

For $n \ge 19$ we obtain $d(n) \le n^\epsilon$ with $\epsilon = 0.988$. Since $p \ge 5$, then $\theta(p) \ge 2-\frac{\pi^2}{5} > 0.026$. We have $n = p^e n_0$ where n_0 is coprime to p. Finally

$$0.026\cdot n\cdot n_0 \le 10^{18p^r}\left(\frac{3}{2}pn^\epsilon+1\right).$$

We have $n_0 \ge 1$ hence $\alpha n \le \beta n^\epsilon + \gamma$ for explicit α, β and γ that depend on p and r only. Such an inequality can hold only for finitely many n. We conclude that there exists a constant $N = N(p,r)$ such that for $n \ge N$ the divisor D_{nP} has a primitive valuation.

For $\chi(S) = h_{K(C)}(E) < 2\cdot p^r(g(C)-1)$ the inequality

$$\frac{\chi(S)}{\widehat{h}_E(P)} \le 10^{36g(C)p^r}.$$

holds. In a similar way as above we obtain a bound $N = N(g(C),p,r)$ such that for $n \ge N$ the divisor D_{nP} has a primitive valuation. □

Remark 8.12. We observe that our leading assumption $p > 3$ is needed to get a positive lower bound on $\theta(p)$. We leave it as an open question whether it is possible to establish the general result that will incorporate prime characteristics 2 and 3.

Let us assume that E is defined over $K(C)$ where the field of constants K of $K(C)$ is not algebraically closed. For $\operatorname{char} K(C) = p$ we put $K = \mathbb{F}_q$ where $q = p^s$ for some positive s. We consider a point P in $E(K(C))$. It is possible to construct the fibration $\pi : S \to C$ such that the generic fibre is E over $K(C)$ and the fibres above $v \in C(\overline{K})$ are defined over the field $k(v)$ which has $\deg v := [k(v) : K]$.

Theorem 8.13. *Let E be an elliptic curve defined over $K(C)$ of characteristic $p > 3$ with field of constants $k = \mathbb{F}_q$, $q = p^s$. Let E be wild. Let $\pi : S \to C$ be an elliptic fibration attached to E in such a way that the fibres E_v above $v \in C(\overline{K})$ of good reduction are defined over $k(v)$. Take a point P in $E(K(C))$ of infinite order. Let p^r be the inseparable degree of the j-map of E. There exists an explicit constant $N = N(g(C), \chi(S), p, r, s)$ which depends only on the genus of C, Euler characteristic $\chi(S)$, p, r and s such that for $n \geq N$ the divisor D_{nP} has a primitive valuation.*

Proof. We proceed in a similar way to the proof of Theorem 8.11. Let n be an integer such that the divisor D_{nP} has no primitive valuation. For $p \nmid n$ we follow the reasoning from the proof of Theorem 8.11. For $p \mid n$, let $e = v_p(n)$. We arrive at the inequality

$$\theta(p) n^2 \widehat{h}_E(P) \leq \frac{3}{2}\chi(S) \cdot (p^{e+1} \cdot d(n)) + \deg W(E, P, n)$$

where $\theta(p)$ is defined as in the proof of Theorem 8.11. For $v \in C(\overline{K})$ of good reduction the fibre E_v is defined over $\mathbb{F}_{q^{\deg v}}$ and the reduction P_v of point P at v is an $\mathbb{F}_{q^{\deg v}}$-rational point. From Lemma 8.1 it follows that $\deg v \leq (p-1)\chi(S)$. Hasse–Weil bound [25, Chap. V, Thm. 1.1] implies that

$$\#E_v(\mathbb{F}_{q^{\deg v}}) \leq \left(\sqrt{q^{\deg v}} + 1\right)^2.$$

From the definition of $m(v)$ we have $m(v) = \operatorname{ord} P_v$, hence

$$m(v) \leq \left(\sqrt{q^{\deg v}} + 1\right)^2 \leq \left(\sqrt{q^{(p-1)\chi(S)}} + 1\right)^2.$$

Let $k = \lceil \log_p(\frac{p+(p-1)^2\chi(S)}{2p-1}) \rceil$ and suppose $e \leq k$. From Lemma 8.9 it follows that

$$\begin{aligned}
&\deg W(E, P, n) \\
&\leq (p^e - 1)\chi(S) + \chi(S) p^{2e} \widehat{h}_E(P) \max\left\{144p^2, (\sqrt{q^{(p-1)\chi(S)}} + 1)^4\right\} \\
&\quad + \frac{1}{2}\chi(S)^2.
\end{aligned}$$

We conclude that there exist explicit constants α, β and γ that depend on $\chi(S), p$ and s such that

$$\theta(p)n^2 \leq \frac{\chi(S)}{\widehat{h}_E(P)}(\alpha d(n) + \beta) + \gamma.$$

We bound trivially $d(n)$ by n from above. When we have

$$\chi(S) \geq 2 \cdot p^r(g(C) - 1)$$

the bound $\frac{\chi(S)}{\widehat{h}_E(P)} \leq 10^{18p^r}$ holds and the inequality is true only for finitely many n under the assumption $p \geq 5$. There is an explicit constant N which depends on $\chi(S), p, s$ and r such that for $n \geq N$ the divisor D_{nP} has a primitive valuation. For $\chi(S) < 2 \cdot p^r(g(C) - 1)$ we produce a constant N that depends additionally on $g(C)$.

Finally, for $e > k$ we find explicit constants α, β, γ that depend on $\chi(S), p$ and s such that

$$\theta(p)n^2 \leq \frac{\chi(S)}{\widehat{h}_E(P)}(\alpha d(n) + \beta)p^e + \gamma p^e.$$

For $n \geq 19$ we have $d(n) \leq n^\epsilon$ with $\epsilon = 0.988$. Now we proceed as in the proof of Theorem 8.11. □

9. Examples

We present several examples where we establish the exact set of nonprimitive divisors for concrete elliptic divisibility sequences. The first example deals with an infinite family of curves in characteristic 0. We prove that as follows from the theorem the constant is absolute and in this case equals 1, i.e. all divisors are primitive.

The second example deals with the curve in characteristic $p = 7$ where the j-map is inseparable. The next three examples indicate what happens when the field $K(C)$ is of positive characteristic and we allow the function $H(E)$ to vanish. We show that there are infinitely many nonprimitive divisors in a sequence. They all rely on the fact that the multiplication by p map is inseparable of degree p^2.

Example 9.1. We present now an example where the constant can be explicitly determined for a large family of elliptic curves with base curve $C = \mathbb{P}^1$ and $\chi(S)$ unbounded. The computations performed in this example inspired the proof of the general case for characteristic 0 fields.

Computations in the example are based on [16]. Let $f, g, h \in \overline{\mathbb{Q}}[t]$ be polynomials of positive degree without a common root that satisfy $f^2 + g^2 = h^2$. We define an elliptic curve

$$E_{f,g,h} : y^2 = x(x - f^2)(x - g^2)$$

over the function field $\overline{\mathbb{Q}}(t)$. There exists a point $Q = (-g^2, \sqrt{-2}g^2h)$ of infinite order on this curve. In the example we present an explicit argument

that for all $n \in \mathbb{N}$ the divisors D_{nQ} are primitive. Note that $\chi(S) = \deg f$ if $\deg g \leq \deg f$ so the Euler characteristic can be made unbounded. We can take for example polynomials

$$(f, g, h) = \left(\frac{t^{2m} - 1}{2}, t^m, \frac{t^m + 1}{2}\right)$$

for any $m \in \mathbb{N}$. The equation $E_{f,g,h}$ represents the globally minimal Weierstrass model of the given elliptic curve. Its fibres of bad reduction are above the points $a \in \overline{\mathbb{Q}}$ such that $f(a) = 0$ or $g(a) = 0$ or $(f^2 - g^2)(a) = 0$ or $a = \infty$. The correcting terms in the Shioda's height formula are recorded in Table 1. We denote by $v_a(\eta)$ the order of vanishing of a polynomial η at a. We also denote $c_v(R, R)$ by $c_v(R)$. The height $\langle Q, Q\rangle$ equals $\deg f$. By the bilinearity of the height pairing $\langle \cdot, \cdot \rangle$ we know that $\langle kQ, kQ\rangle = k^2\langle Q, Q\rangle$. Application of (4.1) implies that

$$k^2\langle Q, Q\rangle = 2\deg f + 2\overline{kQ}.\overline{O} - \sum_{\substack{a:\\ g(a)=0}} c_a(kQ) - c_\infty(kQ).$$

For k even the sum $\sum_{\substack{a:\\ g(a)=0}} c_a(kQ)$ vanishes and for k odd is equal to $\deg g$. Similarly for $2 \mid k$ the factor $c_\infty(kQ)$ equals 0 and for $2 \nmid k$ it is equal to $\deg f - \deg g$. This follows from the group structure of $G(F_v)$ for the fibres under consideration. By a simple algebraic manipulation we get the formula for the intersection numbers

$$\overline{kQ}.\overline{O} = \begin{cases} \frac{k^2-2}{2}\deg f, & 2 \mid k, \\ \frac{k^2-1}{2}\deg f, & 2 \nmid k. \end{cases}$$

Now we compute explicitly the constant $N(E_{f,g,h}, Q)$. Suppose that D_{nQ} does not have a primitive divisors. Then it follows

$$\overline{nP}.\overline{O} \leq \sum_{\substack{m|n\\ m<n}} \overline{mP}.\overline{O}.$$

Suppose n is odd, then

$$\frac{n^2 - 1}{2}\deg f \leq \sum_{\substack{m|n\\ m<n}} \frac{m^2 - 1}{2}\deg f.$$

This is equivalent to

$$(d(n) - 1) + (n^2 - 1) \leq \sigma_2(n) - n^2. \tag{9.1}$$

The first term on the left side of equation (9.1) is nonnegative and $\sigma_2(n) < \zeta(2)n^2$, so

$$n^2 < \frac{1}{2 - \zeta(2)}$$

v	$c_v(Q)$	$\mathrm{comp}_v(Q)$	F_v
∞	$\deg f - \deg g$	$2(\deg f - \deg g)$	$I_{4(\deg f - \deg g)}$
$a : g(a) = 0$	$v_a(g)$	$2v_a(g)$	$I_{4v_a(g)}$
$a : f(a) = 0$	0	0	$I_{4v_a(g)}$
$a : (f^2 - g^2)(a) = 0$	0	0	$I_{2v_a(g)}$

TABLE 1. Correcting terms for a curve with Weierstrass equation $E_{f,g,h}$

hence $n < 1.68$, so $n = 1$. Now we consider the case when n is even. The inequality

$$\frac{n^2-2}{2}\deg f \le \sum_{\substack{m|n\\ m<n}} \overline{mQ}.\overline{O}$$

is equivalent to

$$\left(2d(n) - d\left(n/2^{v_2(n)}\right)\right) + 2(n^2-2) \le \sigma_2(n).$$

We drop the non-negative term $\left(2d(n) - d\left(n/2^{v_2(n)}\right)\right)$. It follows that

$$(2-\zeta(2))n^2 \le 4$$

which can hold only for $n \le 2$. Now we check by a direct computation that D_{2Q} actually contains primitive valuations:

$$2Q = \left(-\frac{(f^2-g^2)^2}{8h^2}, \frac{\sqrt{-1}(g^2-f^2)(3f^2+g^2)(f^2+3g^2)}{16\sqrt{2}h^3}\right)$$

so the constant $N(E_{f,g,h}, Q)$ equals 1.

Example 9.2. Let $C = \mathbb{P}^1$ with parameter t for its function field $K(C)$. Assume that $K = \overline{\mathbb{F}}_7$. The curve $E : y^2 = x^3 - t^3x + t$ has bad reduction at $t = 0$ (type II), $t = 5$ (type I_7) and $t = \infty$ (type III). The associated elliptic surface $\pi : S \to C$ satisfies $\chi(S) = 1$ and hence S is a rational surface with Picard number equal to 10. By Shioda–Tate formula [24, Cor. 5.3] the group $E(\overline{\mathbb{F}}_7(t))$ has rank 1 and by [18] is generated by $P = (3t+2, 2t^2+t+1)$ which has canonical height $\widehat{h}_E(P) = \frac{1}{2}\langle P, P\rangle = \frac{1}{14}$. The four points $P, 2P, 3P$ and $4P$ are integral with respect to t. We prove below that these are the only integral points with respect to t and for all $n \ge 5$ the divisor D_{nP} admits a primitive valuation. Observe that the j-invariant of E is a 7-th power $j = \left(\frac{6t}{t+2}\right)^7$ and its inseparable degree is 7.

We check that for $v \ne 0, \infty$ we have $h_{E,v} = 0$ and $h_{E,0} = 1$, $h_{E,\infty} = 5$, and $m(0) = 7$, $m(\infty) = 14$. Information from Table 3 and knowledge of the

n	D_{nP}
1	0
2	0
3	0
4	0
5	(4)
6	(3)
7	(0)
8	$(\alpha_1) + (\alpha_2)((t-\alpha_1)(t-\alpha_2) = t^2 + 6t + 4$
...	...
14	$(0) + 5(\infty)$

TABLE 2. Divisors D_{nP} for small values of n

v	type of v	P_v	Is singular on E_v?	$c_v(P,P)$
$t=5$	I_7	$(3,0)$	yes	10/7
$t=0$	II	$(2,1)$	no	0
$t=\infty$	III	$(0,0)$	yes	1/2

TABLE 3. Reduction P_v of point P at places v of bad reduction with reduced curve E_v

component group for each bad fibre allow us to compute

$$c_v(kP,kP) = \begin{cases} 1/2 & , v = \infty, 2 \nmid k \\ \frac{(2k \bmod 7)\cdot(7-(2k \bmod 7))}{7} & , v = 5 \\ 0 & , \text{otherwise} \end{cases}$$

We assume $n > 1$ and that D_{nP} has no primitive divisors. From the formula

$$D_{nP} \leq \sum_{\substack{m|n \\ m<n}} p^{v_p(\frac{n}{m})} D_{mP} + W(E,P,n) \tag{9.2}$$

and the computations above we can effectively check that for $5 \leq n \leq 20000$ the formula does not hold. For $n \geq 20000$ we apply the degree function to (9.2) and get

$$0.12n \leq 14 \cdot \left(\frac{31}{24} \cdot n^{0.465} + 1\right)$$

which is valid only for $n \leq 11998$. So only the divisors D_{2P}, D_{3P} and D_{4P} are not primitive and for $n \geq 5$ the divisor D_{nP} always has a primitive valuation. Because $E(\overline{\mathbb{F}}_7(t)) = \langle P \rangle$, so for any $\overline{\mathbb{F}}_7(t)$-rational point Q on E the sequence D_{nQ} contains at most 3 nonprimitive elements.

Example 9.3. Let $p \geq 5$ and pick an elliptic curve $E_0 : y^2 = x^3 + \alpha x + \beta$ with $\alpha, \beta \in \mathbb{F}_p$ which is supersingular. Consider the field $K(C) = \mathbb{F}_p(t)$ of functions of the projective line C over $\mathbb{F}_p$ and let $r = t^3 + \alpha t + \beta$. The curve

$E_0^{(r)} : y^2 = x^3 + \alpha r^2 x + \beta r^3$ over $K(C)$ is a generic fibre of a Kummer K3 surface with I_0^* fibres at places t_0 such that $r(t_0) = 0$ or $t_0 = \infty$. We always have a point $P = (tr, r^2)$ on this curve (in fact $\operatorname{rank} E_0^{(r)}(\overline{\mathbb{F}}_p(t)) = 4$ because E_0 is supersingular, cf.[23, §12.7]). Moreover on E_0 the $[p]$ multiplication map is inseparable of degree p^2 and since E_0 is defined over $\mathbb{F}_p$ we have that $[p](x, y) = (x^{p^2}, -y^{p^2})$. The curve E_0 over $\overline{K(C)}$ is isomorphic to $E_0^{(r^d)}$ over $\overline{K(C)}$ via $(x, y) \mapsto (xr^d, y^{3/2d})$ for any positive integer d. Hence the $[p]$ map on $E_0^{(r)}$ satisfies $[p](x, y) = (x^{p^2} r^{1-p^2}, -y^{p^2} r^{(3-3p^2)/2})$. Any p^k multiple of the point P on $E_0^{(r)}$ is an integral point

$$p^k P = (t^{p^{2k}} r, r^{(3+p^{2k})/2}).$$

The sequence $\{D_{p^k P}\}_{k\geq 0}$ of divisors has support only at $t = \infty$: $D_P = 0$ and $D_{p^k P} = (p^2 - 1)(\infty)$ for $k \geq 1$. Hence the sequence $\{D_{nP}\}_{n\geq 1}$ has infinitely many elements that have no primitive valuation.

There is nothing special about the point P so we can pick any $K(C)$-rational point Q on $E_0^{(r)}$ and there will exist again infinitely many divisors D_{nQ} for $n \geq 1$. From our construction it follows that $H(E) = 0 \in K(C)$.

Example 9.4. Let E be an elliptic curve over $\mathbb{F}_2(t)$ with globally minimal Weierstrass equation

$$E : y^2 + ty = x^3 + x.$$

We consider the point $P = (1, 0)$ which is of infinite order in $E(\mathbb{F}_2(t))$. Multiplication by 2 map on E satisfies the equality

$$x([2](x, y)) = \frac{1 + x^4}{t^2}.$$

For two polynomials p,s in $\mathbb{F}_2[t]$ which are coprime and p/s^2 is the x-coordinate a point Q on E we get

$$x(2Q) = \frac{p^4 + s^8}{t^2 s^8}$$

and it is easy to see that $p^4 + s^8$ and $t^2 s^8$ are again coprime. We show by induction that for $l \geq 1$

$$x(2^l P) = \frac{\sum_{j=1}^{l-1} t^{\sum_{k=j}^{l-2} 2^{2k+1}}}{t^{\frac{2}{3}(2^{2l-2}-1)}}.$$

So for $l \geq 2$ we have $\operatorname{Supp} D_{2^l P} = \{(0)\}$ and for every $l \geq 3$ the divisor $D_{2^l P}$ is not primitive.

Example 9.5. Let E be an elliptic curve over $\mathbb{F}_3(t)$ with globally minimal Weierstrass equation

$$E : y^2 + txy = x^3 + 2t^2 x^2 + (2t^2 + 1)x + (2t^2 + 1).$$

The point $P = (1, 0)$ is of infinite order in $E(\mathbb{F}_3(t))$. We check that

$$x([3](x, y)) = \frac{1}{(1+t)^4(2+t)^4}x^9 + \frac{2t^2}{(1+t)(2+t)}.$$

For $l \geq 1$ the divisor $D_{3^l P}$ is supported at 1 and 2 and for $l \geq 2$ it is not primitive.

Acknowledgments

The author would like to thank Wojciech Gajda for suggesting this research problem and for the hint to the height bounds of [9] used at the critical point of the argument. He also thanks Krzysztof Górnisiewicz for helpful remarks, Maciej Radziejewski for his information about the upper bounds on the divisor sum functions and Joseph Silverman for helpful comments. Finally the author thanks an anonymous referee for careful reading of the manuscript and for very helpful suggestions.

References

[1] Cossec, François R.; Dolgachev, Igor V. Enriques surfaces. I. Progress in Mathematics, 76. *Birkhäuser Boston Inc., Boston, MA*, 1989. x+397 pp. ISBN: 0-8176-3417-7. MR0986969, Zbl 0665.14017, doi: 10.1007/978-1-4612-3696-2.

[2] Elkies, Noam D. Points of low height on elliptic curves and surfaces. I. Elliptic surfaces over $\mathbb{P}^1$ with small d. *Algorithmic number theory*, 287–301, Lecture Notes in Comput. Sci., 4076. *Springer, Berlin*, 2006. MR2282931, Zbl 1143.11334, arXiv:math/0608593, doi: 10.1007/11792086.

[3] Everest, Graham; Ingram, Patrick; Mahé, Valéry; Stevens, Shaun. The uniform primality conjecture for elliptic curves. *Acta Arith.* **134** (2008), no. 2, 157–181. MR2429645, Zbl 1246.11117, arXiv:0712.2696, doi: 10.4064/aa134-2-7.

[4] Everest, Graham; Ingram, Patrick; Stevens, Shaun. Primitive divisors on twists of Fermat's cubic. *LMS J. Comput. Math.* **12** (2009), 54–81. MR2486632 (2010b:11060), Zbl 1252.11049, arXiv:math/0703553, doi: 10.1112/S1461157000000024.

[5] Everest, Graham; Mclaren, Gerard; Ward, Thomas. Primitive divisors of elliptic divisibility sequences. *J. Number Theory* **118** (2006), no. 1, 71–89. MR2220263, Zbl 1093.11038, arXiv:math/0409540, doi: 10.1016/j.jnt.2005.08.002.

[6] Everest, Graham; Reynolds, Jonathan; Stevens, Shaun. On the denominators of rational points on elliptic curves. *Bull. Lond. Math. Soc.* **39** (2007), no. 5, 762–770. MR2365225, Zbl 1131.11034, doi: 10.1112/blms/bdm061.

[7] Flatters, Anthony; Ward, Thomas. A polynomial Zsigmondy theorem. *J. Algebra* **343** (2011), 138–142. MR2824548, Zbl 1257.11028, arXiv:1002.4829, doi: 10.1016/j.jalgebra.2011.07.010.

[8] Hartshorne, Robin. Algebraic geometry. Graduate Texts in Mathematics, 52. *Springer-Verlag, New York-Heidelberg*, 1977. xvi+496 pp. ISBN: 0-387-90244-9. MR0463157, Zbl 0367.14001, doi: 10.1007/978-1-4757-3849-0.

[9] Hindry, M.; Silverman, J. H. The canonical height and integral points on elliptic curves. *Invent. Math.* **93** (1988), no. 2, 419–450. MR0948108, Zbl 0657.14018, doi: 10.1007/BF01394340.

[10] Ingram, Patrick. Elliptic divisibility sequences over certain curves. *J. Number Theory* **123** (2007), no. 2, 473–486. MR2301226, Zbl 1170.11010, doi: 10.1016/j.jnt.2006.08.007.

[11] Ingram, Patrick; Mahé,Valéry; Silverman, Joseph H.; Stange, Katherine E; Streng, Marco. Algebraic divisibility sequences over function fields. *J. Aust. Math. Soc.* **92** (2012), no. 1, 99–126. MR2945679, Zbl 1251.11008, arXiv:1105.5633, doi: 10.1017/S1446788712000092.

[12] Ingram, Patrick; Silverman, Joseph H. Uniform estimates for primitive divisors in elliptic divisibility sequences. *Number theory, analysis and geometry*, 243–271. *Springer, New York*, 2012. MR2867920, Zbl 1276.11092, doi: 10.1007/978-1-4614-1260-1_12.

[13] Katz, Nicholas M. p-adic properties of modular schemes and modular forms. *Modular functions of one variable, III* (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), pp. 69–190. Lecture Notes in Mathematics, 350. *Springer, Berlin*, 1973. MR0447119, Zbl 0271.10033, doi: 10.1007/978-3-540-37802-0_3.

[14] Katz, Nicholas M.; Mazur, Barry. Arithmetic moduli of elliptic curves. Annals of Mathematics Studies, 108. *Princeton University Press, Princeton, NJ*, 1985. xiv+514 pp. ISBN: 0-691-08349-5; 0-691-08352-5. MR0772569, Zbl 0576.14026, doi: 10.1515/9781400881710.

[15] Kühn, Ulf; Müller, Jan Steffen. A height inequality for rational points on elliptic curves implied by the *abc*-conjecture. *Funct. Approx. Comment. Math.* **52** (2015), no. 1, 127–132. MR3326129, Zbl 06425018, arXiv:1210.6543, doi: 10.7169/facm/2015.52.1.10.

[16] Naskręcki, Bartosz. Mordell–Weil ranks of families of elliptic curves parametrized by binary quadratic forms. Preprint, 2015, arXiv:1609.04715.

[17] Nicolas, J.-L.; Robin, G. Majorations explicites pour le nombre de diviseurs de N. *Canad. Math. Bull.* **26** (1983), no. 4, 485–492. MR0716590, Zbl 0497.10034, doi: 10.4153/CMB-1983-078-5.

[18] Oguiso, Keiji; Shioda, Tetsuji. The Mordell–Weil lattice of a rational elliptic surface. *Comment. Math. Univ. St. Paul.* **40** (1991), no. 1, 83–99. MR1104782, Zbl 0757.14011.

[19] Pesenti, J.; Szpiro, L. Inégalité du discriminant pour les pinceaux elliptiques à réductions quelconques. *Compositio Math.* **120** (2000), no. 1, 83–117. MR1738213, Zbl 1021.11021, doi: 10.1023/A:1001736823128.

[20] Reynolds, Jonathan. Perfect powers in elliptic divisibility sequences. *J. Number Theory* **132** (2012), no. 5, 998–1015. MR2890523, Zbl 1276.11094, arXiv:1101.2949, doi: 10.1016/j.jnt.2011.09.013.

[21] Roquette, Peter. Analytic theory of elliptic functions over local fields. Hamburger Mathematische Einzelschriften (N.F.), Heft 1. *Vandenhoeck & Ruprecht, Göttingen*, 1970. 90 pp. MR0260753, Zbl 0194.52002.

[22] Rosser, J. Barkley; Schoenfeld, Lowell. Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$. *Math. Comp.* **29** (1975), 243–269. MR0457373, Zbl 0295.10036, doi: 10.2307/2005479.

[23] Schütt, Matthias; Shioda, Tetsuji. Elliptic surfaces. *Algebraic geometry in East Asia–Seoul 2008*, 51–160, Adv. Stud. Pure Math., 60. *Math. Soc. Japan, Tokyo*, 2010. MR2732092, Zbl 1216.14036, arXiv:0907.0298.

[24] Shioda, Tetsuji. On the Mordell–Weil lattices. *Comment. Math. Univ. St. Paul.* **39** (1990), no. 2, 211–240. MR1081832, Zbl 0725.14017.

[25] Silverman, Joseph H. The arithmetic of elliptic curves. Graduate Texts in Mathematics, 106. *Springer-Verlag, New York*, 1986. xii+400 pp. ISBN: 0-387-96203-4. MR0817210, Zbl 0585.14026.

[26] Silverman, Joseph H. Wieferich's criterion and the *abc*-conjecture. *J. Number Theory* **30** (1988), no. 2, 226–237. MR0961918, Zbl 0654.10019, doi: 10.1016/0022-314X(88)90019-4.

[27] Silverman, Joseph H. Advanced topics in the arithmetic of elliptic curves. Graduate Texts in Mathematics, 151. *Springer-Verlag, New York*, 1994. xiv+525 pp. ISBN: 0-387-94328-5. MR1312368, Zbl 0911.14015, doi: 10.1007/978-1-4612-0851-8.

[28] Silverman, Joseph H. Common divisors of elliptic divisibility sequences over function fields. *Manuscripta Math.* **114** (2004), no. 4, 431–446. MR2081943, Zbl 1128.11015, arXiv:math/0402016, doi: 10.1007/s00229-004-0468-7.

[29] Stange, Katherine. Elliptic nets and elliptic curves. *Algebra Number Theory* **5** (2011), no. 2, 197–229. MR2833790, Zbl 1277.11063, arXiv:0710.1316, doi: 10.2140/ant.2011.5.197.

[30] Stange, Katherine E. Integral points on elliptic curves and explicit valuations of division polynomials. *Canad. J. Math.* **68** (2016), no. 5, 1120–1158. MR3536930, arXiv:1108.3051, doi: 10.4153/CJM-2015-005-0.

[31] Streng, Marco. Divisibility sequences for elliptic curves with complex multiplication. *Algebra Number Theory* **2** (2008), no. 2, 183–208. MR2377368, Zbl 1158.14029, doi: 10.2140/ant.2008.2.183.

[32] Tate, John. Algorithm for determining the type of a singular fiber in an elliptic pencil. *Modular functions of one variable, IV* (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), pp. 33-52, Lecture Notes in Math., 476. *Springer, Berlin*, 1975. MR0393039, Zbl 1214.14020, doi: 10.1007/BFb0097582.

[33] Tate, John. A review of non-Archimedean elliptic functions. *Elliptic curves, modular forms, & Fermat's last theorem* (Hong Kong, 1993), 162–184, Ser. Number Theory, I. *Int. Press, Cambridge, MA*, 1995. MR1363501, Zbl 1071.11508.

[34] Ward, Morgan. The law of repetition of primes in an elliptic divisibility sequence. *Duke Math. J.* **15** (1948), 941–946. MR0027286, Zbl 0032.01403, doi: 10.1215/S0012-7094-48-01582-8.

[35] Ward, Morgan. Memoir on elliptic divisibility sequences. *Amer. J. Math.* **70** (1948), 31–74. MR0023275, Zbl 0035.03702, doi: 10.2307/2371930.

(Bartosz Naskręcki) Faculty of Mathematics and Computer Science, Adam Mickiewicz University, Umultowska 87, 61-614 Poznań, Poland, and School of Mathematics, University of Bristol, University Walk, Bristol BS8 1TW, UK
nasqret@gmail.com

This paper is available via http://nyjm.albany.edu/j/2016/22-46.html.